ACT Research & Policy

Issue Brief

October 2014

Although shifting to computer administration of tests does reduce some test security risks, it also creates new risks that states will need to address with new laws and policies.

The End of Erasures: Updating Test Security Laws and Policies for Computerized Testing

Michelle Croft

In 2013, 35 educators in Atlanta, including the district superintendent, were indicted for cheating on the state's standardized tests with charges ranging from making false statements to racketeering.[1] The cheating activities were alarming: educators meeting over the weekend to erase and correct incorrect answers, arranging classroom seating so lower ability students could see the answer sheets of higher ability students, and looking at the next day's test questions and discussing the questions with the class.[2] In January 2014, eight of the educators pleaded guilty,[3] and the trial for twelve others started in August 2014.[4]

The actions in Atlanta are not anomalous. In Philadelphia three high school principals were fired and 130 other educators face disciplinary actions for cheating on student assessments.[5] Cheating scandals have surfaced across the country in California, Arizona, Michigan, Ohio, Florida, and Washington, DC.

In the wake of these test security scandals, strong test security measures are needed given the importance of scores for instruction, evaluation, and accountability. In 2012, the National Center for Education Statistics (NCES) held a symposium to discuss best practices related to prevention, detection, and investigation of testing irregularities.[6] Since most states are moving away from paper-and-pencil test administration,[7] one of the topics discussed was the transition to computer-administered testing. This shift to computer administration could be seen as a way to avoid many of the test security problems at issue in cities like Atlanta and Washington, DC. In those cities, most of the media attention focused on the high number of wrong-to-right erasures, where more students' answer documents had more changes from wrong to right than would statistically be expected. With computerized testing, there are no testing booklets or answer sheets.

Computerized test administration, however, introduces its own test security risks. A panelist at the NCES symposium highlighted that "shifting to a new assessment delivery model such as a computer delivered or even computer adaptive testing does not make cheating and test piracy go away. They merely take a different form."[8] For instance, many of the test security concerns will be the same. There will still need to be efforts to prevent unauthorized access to secure exam materials, student access to restricted materials (e.g., a calculator when not allowed for testing), or inappropriate use of accommodations. There are unique risks for test security breaches depending on the delivery mode. For computerized administration, such risks include:[9]

- educators logging in to tests to view questions or change student responses
- computer hacking
- keystroke logging
- printing, emailing, or storing test information in a computer outside the test delivery system

Furthermore, compared to paper-and-pencil administration, there is a greater risk of students accessing the Internet and other programs during testing.[10] These security risks are increased when students are allowed to test on their own

Email research.policy@act.org for more information.

devices, as in bring-your-own-device (BYOD) testing, or when students or educators have administrative privileges on the device; such circumstances may allow students or educators to interfere with locked-down test delivery environments.[11]

Given the transition from paper-and-pencil to computer administration, policymakers must update test security laws and policies to reflect the new threats to administration. In a 2013 review of state test security statutes and regulations, I found that the laws are primarily oriented toward paper-and-pencil assessment.[12] Although there are certain provisions that apply equally to both modes of administration (e.g., preventing access to items prior to testing or inappropriate use of accommodations),[13] the laws were heavily focused on paper-and-pencil assessment security issues related to details about storage, access, and establishing a chain of custody. Only two states—Delaware and Oregon—had information in their state statutes and regulations specific to computer administration.[14]

There will likely always be a need for paper-and-pencil test administration security laws and policies, given that paper test copies may be needed as an accommodation or may be needed in places with limited technology infrastructure. However, it is necessary for states to augment their current test security laws and policies to account for the changes in test security needs.

The question, then, is what should be included in those laws and policies? This paper suggests ways states can update their statutes, regulations, and policy manuals to reflect the shift to computer administered testing.

What States Are Doing

In 2011, the State Educational Technology Directors Association (SETDA) published a list of state assessment technology requirements.[15] The report included the first year each state offered online testing in any subject for any population and whether the assessments the state offers are mandatory, voluntary, or both (a state may require computer administration at the high school level but not at the elementary school level). To identify computer-specific test security practices, I selected states that administered at least one mandatory computer-administered assessment. Sixteen states met the criteria. I then reviewed each state's assessment administration manual's test security section and other relevant portions of the manual. Six common themes emerged from the manuals: storage and secure materials, test access, testing window, student workstations, technology requirements, and specificity. In what follows, each of these themes is discussed with examples.

Storage and Secure Materials

Because there will likely always be paper-and-pencil forms as an accommodation for certain students with disabilities, the inclusion of paper-and-pencil test security policies, particularly those policies related to storage, is appropriate. Computer-based testing does not eliminate the need to focus on the security of materials, however, since students often are provided with "tickets" to gain admission to the test. The student ticket may include the student's name and login information. This information must be secure so someone other than the student does not use the login information to access the test either to gain knowledge of the test items or to complete the test on the student's behalf. Likewise, scratch paper may be kept secure prior to and after testing.

The storage provisions traditionally reserved for paper-and-pencil tests can be adapted for computer-based testing. For instance, the test security portion of Florida's manual refers to "secure materials," which are later defined to include work folders, student authorization tickets, and session rosters.[16] The key is to explicitly define which materials are secure and ensure that all necessary items for computer-based testing (such as test tickets) are included. As an example, Idaho's manual specifically lists scratch paper, reference sheets, and test session tickets as secure testing materials within its test security section.[17]

In addition to adapting the paper-and-pencil materials storage policies to include the

Statutes, Regulations, and Policies

States have several options for establishing law and policy related to test security, each with its own advantages and disadvantages.

Statutes are laws enacted by the state's legislature and have the ultimate authority. Because it takes legislative action to change a statute, these are generally broad and grant authority to the state's department of education to work out details through regulation or policy.

Regulations are developed by the state agency to build upon the statutory framework and provide more detail. The regulations cannot contradict statutes and have the force of law after public notice and comment.

Policies are also developed by the state agency, but without notice and comment. Policies may not contradict statutes or regulations. Because they can be developed without legislative or public approval, they can be changed most easily.

paper components related to computer administration, there can be protections to safeguard student login information in addition to locked storage. For instance, in Oregon it is a violation to send a student's name and student ID together in an email or to otherwise provide a student's login information to someone other than the student.[18] Likewise, West Virginia schools are able to print the test tickets on the day of testing and avoid having to securely store the tickets prior to testing.[19]

Test Access

Computer-based testing does not eliminate the problem of someone other than the student completing the test, as was highlighted with the secure nature of the student test ticket. States must have policies describing who can access the tests and under what conditions. For instance, Minnesota explicitly mentions that—absent a specific accommodation—students must enter their own responses.[20]

The policies should first start by defining who should have access to a student's login information. As mentioned previously, states classify login information as secure.[21] In Delaware, it is a specific assessment behavior violation to intentionally give students the incorrect login.[22]

The challenge arises when students have difficulty logging in to the test system or when a student logs out mid-test. In Florida, test administrators can help with login errors, but they are not allowed to attempt to resolve an issue once testing has begun.[23] If a student exits the test, the proctor can resume the test.[24] Kansas has a detailed system for reactivations. If a student needs a test reactivated, two people should be present and the proctor should keep a log of all reactivations.[25] Reactivations are limited to situations when a student's final score has not been posted.[26]

Testing Window

The testing window is the amount of time available for testing within a school or district. With paper-and-pencil assessments, testing windows can be as short as two weeks, which allows a week for testing and a week for retesting students who were not present the first week. For computer-based testing, the testing window generally needs to be longer to accommodate for the often limited number of computers available for testing. The testing window has test security implications because the likelihood of item exposure increases the longer the testing window is open.

Indiana clearly identifies the issue of the testing window. The Indiana manual provides different test windows based on mode of administration. For paper-and-pencil administrations, each test session is to be administered at the same time to all students in a grade, whereas for computer-based administrations, each test session should be administered at the same time to all students in a class.[27] These practices help to limit the chance that tested students will discuss items with their yet-to-be-tested classmates.

Student Workstations

Another test security issue is the ability of others to see a student's test and responses. Given that it may be easier to see test items and student responses on a computer screen than on a traditional paper booklet and answer sheet, the layout of student workstations increases in importance with computerized testing. States such as Missouri, Florida, Oregon, and Virginia recommend visual barriers or adequate spacing between workstations so that students cannot see one another's screens.[28] Oklahoma takes the recommendation further and requires that no one other than the student taking the test is allowed to view the student's screen after testing starts.[29]

Technology

The security of the technology is vital for computer administration. Many of the test security threats unique to computer-based administration are due to threats such as computer hacking, keystroke logging, or managing to get test information outside of the test delivery system (e.g., printing, emailing, or otherwise storing the test on the computer). Some of these threats to test security are dealt with through the test contractor and the testing platform. But there are steps states have taken to reduce technological threats to test security. Some suggested state practices include prohibiting access to the Internet during testing,[30] turning off monitoring software that would allow test content to be viewed on another computer during testing,[31] or having a secure browser or Internet connection.[32]

Specificity

All of the manuals have test security sections. The specificity of the test security sections varies greatly by state, particularly when differentiating between paper-and-pencil and computer-based administrations.

Some manuals only contain very general test security provisions that do not address computer administration. Instead, relevant test security information is included throughout the manual. For example, in Florida the test security portion of the manual refers to "secure materials" but does not define what other materials are secure other than test and answer books.[33] One has to read the remainder of the manual to discover that used work folders, student authorization tickets, and session rosters are also required to be secure.[34]

Some states clearly articulate test security policies related to computerized testing. Kansas, for example, designates student test tickets and paper copies of assessments as secure materials and includes information about best practices for reactivating tests.[35]

Recommendations

The shift to computer administration reduces certain test security risks but creates new risks that need to be addressed through statutes, regulations, or policies. In addition to the challenges and solutions mentioned above, what can states do to prevent computer-based assessment security breaches? Three steps are most immediate:

1. **States should update their state statutes and regulations to reflect the shift to computer-administered assessment.** State statutes and regulations set up a framework for the policy guidance in the test administration manual. The statutes and regulations should acknowledge that there are distinct risks to test security based on administration mode. The statutes and regulations are not the appropriate tools for including specific technical information (such as the types of devices that may be used and the specific browser requirements), but they do signal to districts and educators that test security problems do not disappear with the transition to computer administration.
2. **Concentrate efforts on controlling test access.** Like paper-and-pencil administration, computer-based administration requires controlling access to the test. With paper-and-pencil administrations the challenge was controlling access to the test items primarily before the test was administered and the answer sheets after administration. With computer-based administration, the access problem remains. States should consider policies that keep student login information secure and have rules about how tests are reactivated in the event a test is disrupted. The rules should emphasize having more than one proctor aid in the reactivation, and most importantly, proctors should maintain a log of all reactivations to provide documentation in the event of an investigation. Likewise, the technology should be secure and the testing window should be as short as possible to reduce the likelihood that items are compromised. Finally, states should actively monitor test access issues through data reports to determine if there have been excessive logins or logins at times when testing should not occur (e.g., on the weekends), and have clear policies in place detailing how violations will be handled.
3. **When updating the test administration manuals, the test security section should have all necessary information.** The test security section of the manual should be the "one-stop shop" for any question that a test administrator has about test security. At a minimum, there should be an itemized list of what materials are secure. Information about who can access the test should be clearly articulated. In addition, there should be information on how to report test security concerns and possible violations, which can be applicable regardless of the testing format. ■

Notes

1 Michael Winerip, "Ex-Schools Chief in Atlanta Is Indicted in Testing Scandal," *New York Times* (March 29, 2013), http://www.nytimes.com/2013/03/30/us/former-school-chief-in-atlanta-indicted-in-cheating-scandal.html?pagewanted=all&_r=0; and Lesli A. Maxwell, "Former Atlanta Educators Plead Guilty Over Cheating," *Education Week* (January 8, 2014).

2 Michael J. Bowers, Robert E. Wilson, and Richard L. Hyde, *Atlanta Public School System Investigative Report* (Atlanta, GA: Office of the Governor Special Investigators, 2011), http://graphics8.nytimes.com/packages/pdf/us/Volume-1.pdf.

3 Winerip, "Ex-Schools Chief in Atlanta Is Indicted in Testing Scandal," *New York Times*; and Maxwell, "Former Atlanta Educators," *Education Week*.

4 Mark Niesse and Bill Rankin, "Atlanta Schools Test-Cheating Trial Begins," *Atlanta Journal Constitution* (August 11, 2014).

5 Lesli A. Maxwell, "Philadelphia Cheating Probe Implicates More Than 130 Educators," *Education Week* (January 21, 2014).

6 National Center for Education Statistics, *Testing Integrity Symposium: Issues and Recommendations for Best Practice* (Washington, DC: National Center for Education Statistics, 2013).

7 As of May 2014 there were 17 states participating in the PARCC testing consortium and 22 states in Smarter Balanced Assessment Consortium. Both consortia will be using computer administrations of their tests.

8 National Center for Education Statistics, *Testing Integrity Symposium*, 16.

9 John F. Olsen and John Fremer, *TILSA Test Security Guidebook: Preventing, Detecting, and Investigating Test Security Irregularities* (Washington, DC: CCSSO, 2013), 16.

10 National Center for Education Statistics, *Testing Integrity Symposium*, 15–18.

11 Dian Schaffhauser, "As High-Stakes Online Testing Approaches, Will Your iPads Work?" *The Journal* (September 2012), accessed July 9, 2014, http://thejournal.com/Articles/2012/10/11/You-May-Now-Open-Your-Test-Tablets.aspx.

12 Michelle Croft, *A Review of State Test Security Laws in 2013*, ACT Research Report Series 2014-1 (Iowa City, IA: ACT, 2014).

13 Olsen and Fremer, TILSA *Test Security Guidebook*, 16

14 The report only analyzed state statutes and regulations, not state test administration manuals, which would likely contain additional information about computer administration and test security.

15 State Educational Technology Directors Association (SETDA), *Technology Requirements for Large-Scale Computer-Based and Online Assessment: Current Status and Issues* (Glen Burnie, MD: SETDA, 2011), http://www.setda.org/wp-content/uploads/2014/03/large-scale_techrequirements_june22_combined.pdf.

16 Florida Department of Education, *2013–2014 End-of-Course Assessments* (Tallahassee, FL: Florida Department of Education, 2013), 10 and 146.

17 Idaho State Department of Education, *Idaho Standards Achievement Tests Test Administration Manual Spring 2014* (Boise, ID: Idaho State Department of Education, 2014), http://isat.caltesting.org/docs/2014/ISAT_Spring2014_TAM.pdf.

18 Oregon Department of Education, *Test Administration Manual 2013–2014 School Year* (Salem, OR: Office of Student Assessment and Information Services, Oregon Department of Education, 2013–2014), 15.

19 West Virginia Department of Education, *2014 WESTEST 2 Administration Manual* (Charleston, WV: West Virginia Department of Education, 2014).

20 Minnesota Department of Education, *2013–2014 Title I Assessment Manual* (Roseville, MN: Minnesota Department of Education, 2014), http://www.mnstateassessments.org/wp-content/uploads/2013/07/2013-14_TITLE_1Manual_5081.pdf.

21 Hawaii also classifies logins as secure under federal privacy laws and makes it an assessment violation to log in using a different ID. Hawai'i Statewide Assessment Program, *Hawai'i Statewide Assessment Program (Online HAS and End-of-Course Exams Test Administration Manual 2013–2014* (Honolulu, HI: Hawaii State Department of Education, 2013–2014) 13, http://alohahsap.org/EOC/wp-content/uploads/HI_TAM_2013_2014.pdf.

22 Delaware Comprehensive Assessment System, *Online Test Administration Manual* (Dover, DE: Delaware Department of Education, 2013), 14, http://de.portal.airast.org/wp-content/uploads/2013/06/DCAS_Online_Test_Admin_Manual_2013-14.pdf.

23 Florida Department of Education, *2013–2014 End-Of-Course Assessments*, 7.

24 Florida Department of Education, *2013–2014 End-Of-Course Assessments*, 36.

25 Kansas State Department of Education, *Kansas Assessment Examiner's Manual 2013–14* (Topeka, KS: Kansas State Department of Education, 2014), http://www.ksde.org/Portals/0/CSAS/CSAS%20Home/Assessments/KSExamManual2014.pdf.

26 There is an exception "for students who have not answered all test questions contained within a test section as noted on the Missing Responses page provided by [Center for Educational Testing & Evaluation]." Kansas State Department of Education, *Kansas Assessment Examiner's Manual*, 6.

27 Indiana Department of Education, *Chapter Ten: Test Administration, Test Security, and Reporting* (Indianapolis, IN: Indiana Department of Education, 2014), 5, http://www.doe.in.gov/sites/default/files/assessment/chapter-10-test-preparation-administration-and-reportingfinal4-17-14.pdf.

28 Missouri Department of Elementary & Secondary Education, *End-of-Course Assessments Test Administration Manual 2013–2014* (Jefferson County, MO: Missouri Department of Education, 2013), 6, http://dese.mo.gov/sites/default/files/asmt-eoc-test-administration-manual.pdf; Florida Department of Education, *2013–2014 End-Of-Course Assessments*, 26; Oregon Department of Education, *Test Administration Manual*, 11; and Virginia Department of Education, *Virginia Standards of Learning Assessments*, 4.

29 Oklahoma State Department of Education, *Oklahoma School Testing Program Online Test Administration Manual 2013–2014* (Monterey, CA: CTB/McGraw-Hill LLC, 2014), 3, http://www.ctb.com/netcaster/ncmedia/15163/2706012-W_EOIen_TAM-OL_s14OC.pdf.

30 Hawai'i Statewide Assessment Program, *Hawai'i Statewide Assessment Program*.

31 Florida Department of Education, *2013–2014 End-Of-Course Assessments*, 19.

32 Oregon Department of Education, *Test Administration Manual*; Virginia Department of Education, *Virginia Standards of Learning Assessments Examiner's Manual Fall 2013, Spring 2014, & Summer 2014* (Richmond, VA: Virginia Department of Education, 2013), http://www.doe.virginia.gov/testing/test_administration/manuals/examiners/non-writing/nonwriting_eoc_mathematics.pdf.

33 Florida Department of Education, *2013–2014 End-of-Course Assessments*.

34 Florida Department of Education, *2013–2014 End-Of-Course Assessments*, 10 and 146.

35 Kansas State Department of Education, *2013–2014 Kansas Assessment Examiner's Manual*.